IN THE UNITED STATES DISTRICT COURT FOR THE NORTHERN DISTRICT OF GEORGIA

FERROVIAL CONSTRUCTION US CORP., ET AL.; Plaintiffs, VERSUS JESUS GONZALEZ FERNANDEZ, ET AL., Defendants.	CIVIL ACTION NO. 1:25-CV-0804-LMM

PLAINTIFFS' OPPOSITION TO DEFENDANTS' MOTION TO DISMISS

Plaintiffs oppose Defendants' Rule 12(b)(6) *Motion to Dismiss* [ECF No. 69] (the "MTD"), which the Court should deny for the reasons set forth below.[1]

[1] The term "Plaintiffs" has been previously defined. So, too, has the term "Defendants," which includes Plaintiffs' former high-ranking employees (now referred to as "Individuals") and their new employer and Plaintiffs' competitor, Acciona. Citations to the "MTD" are to ECF No. 69-1, the Brief in Support.

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page(s)

Cases

PRELIMINARY STATEMENT

On May 15, 2025, the Court indicated, based on its review of the *First Amended Complaint* (the "FAC") and *Motion for Preliminary Injunction*, that expedited forensic discovery is warranted to determine to what extent Plaintiffs' trade secrets migrated to the Individuals' Acciona laptops. Following this conference, Defendants agreed in a *Consent Order* not to use Plaintiffs' trade secrets "identified or referenced in" the FAC, which shows that—contrary to what they allege in the MTD—Defendants know perfectly well what information forms the basis of Plaintiffs' claims (otherwise, how could they agree not to use it?).[2] Then, on June 25, 2025, Defendants agreed to a heavily negotiated *Forensic Protocol* designed to granularly identify files containing Plaintiffs' trade secrets residing on Acciona's computers.

Their apparent knowledge notwithstanding, Defendants nevertheless filed their MTD attacking the sufficiency of Plaintiffs' allegations, on four main grounds, all of which lack merit. ***First***, they argue that Plaintiffs have alleged insufficient facts to establish "reasonable measures" taken under the circumstances to protect their

[2] The *Consent Order* is neither an admission of liability nor a waiver of rights or defenses. Plaintiffs use of it, here—to show that Defendants must know what information is at issue—implicates neither admission nor waiver.

trade secrets. In advancing this argument, Defendants improperly invite premature factual determinations; ignore key, detailed allegations that satisfy Rule 12's relaxed standard; uncritically cite distinguishable cases; and ignore cases that directly contradict their position.

Second, Defendants argue that Plaintiffs must do more to identify their trade secrets with "sufficient particularity"; but this argument rests solely on a heightened pleading standard that plainly doesn't exist. But, even were the Court to indulge this fictitious pleading standard, Plaintiffs would prevail regardless, having identified their trade secrets with "sufficient particularity," going as far as identifying specific files, folders, and external storage devices that contain them.

Third, Defendants argue that Plaintiffs have failed to establish improper acquisition or misuse of trade secrets. In this, too, Defendants ignore Plaintiffs' well-pled allegations that the Individuals—acting in concert with Acciona—secretly downloaded, without authorization, thousands of files containing trade secrets shortly before their resignations, including after they accepted employment with Acciona, and then accessed and/or used that information to benefit themselves and Acciona, all while concealing their efforts.

Fourth, Defendants argue that Plaintiffs have also failed to establish that Acciona is liable the misconduct pled herein. Acciona contends that when trusted employees engage in suspicious computing activity, only to join a competitor in the

same roles, and then use secreted information with their new employer's knowledge and for its benefit, that new employer is somehow immune. Unsurprisingly, this is not the law; and Plaintiffs have pled sufficient facts to state direct claims against Acciona and, also, to impose liability on Acciona for the misconduct of the Individuals, its agents.

RELEVANT FACTUAL ALLEGATIONS[3]

The FAC is replete with allegations that plausibly establish Plaintiffs' trade secret claims. Plaintiffs design, develop, and build large-scale infrastructure projects. *See* FAC ¶ 2. They compete against Acciona, with both companies often bidding against one another for the same major projects. *See id.* ¶¶ 1, 3, 43, 45. The Individuals joined Acciona improperly, in that – as part of their departures – they misappropriated Plaintiffs' trade secrets, only to disclose those secrets after starting with Acciona, and then actively conceal their actions. *See id.*, ¶¶ 4-13, 47-58, 62-92, 99-102. The Individuals, moreover, were not ordinary employees. Each was long-tenured in a position of authority and trust; and all had access to Plaintiffs' trade secrets. *See id.* ¶¶ 3, 7, 9, 60-61, 69, 73-74, 76, 98.

Reasonable Measures. Long-tenured, high-ranking, and trusted employees like the Individuals should know better than to surreptitiously download and retain trade

[3] Plaintiffs do not reproduce each of the FAC's 100-plus allegations. They focus on those that, together and with all inferences they create, defeat the MTD.

secrets—shortly before resigning and after accepting new employment—for the benefit of their new employer. Regardless, and as stated in the FAC, Plaintiffs took (and still take) "reasonable measures" to "protect," "safeguard," and "preserve the secrecy" of the trade secrets to which the Individuals had access:

- ". . . Plaintiffs require employees to agree to be bound by [an Ethics Code] that states: 'Ferrovial's . . . confidential information is one of its greatest assets,' which includes '[t]echnical information, designs, process data, pricing information, strategic plans, know-how, software and technology.' It further states that employees 'should never use Ferrovial's confidential information . . . outside the scope of the professional context in which it was originally obtained' and that 'Ferrovial's property should never be used . . . to further the activities of a competitor.'" *Id.* ¶ 32.

- "Employees also agree to be bound by the 'Procedure for the Use of Technological Resources,' which serves the purpose of 'safeguarding the integrity, confidentiality, and availability[‘] of Ferrovial's information; and the 'Competition Policy," which specifically prohibits the exchange of confidential business information among competitors." *Id.* ¶ 33.

- ". . . even to accomplish the everyday task of simply logging into their computer, [the Individuals] (like all employees with access to Ferrovial's computing network) were required to acknowledge and agree that their access was granted for the limited purpose of performing work for Ferrovial and was given subject to compliance with the Procedure for the Use of Technological Resources." *Id.* ¶ 33.

- "Plaintiffs protect their confidential information on password-protected internal computer servers that can only be accessed by select employees who have a valid reason to review or use [it]. . . Plaintiffs also train their employees . . . that [these data] are confidential and valuable . . . and may not be disclosed to anyone outside of [Plaintiffs]. And . . . Plaintiffs are able to monitor employees' computing activity . . . to safeguard their trade secrets." *Id.* ¶ 35.

The FAC attaches these policies and alleges that each of the Individuals was "bound

by [them] during their employment." FAC, ¶ 34; *see also* ECF Nos. 9-5—9-7.[4]

Reasonable Identification. Plaintiffs adequately detailed (i) the specific dates the misappropriations occurred; (ii) the specific external devices—often by serial number—used; (iii) the types of files misappropriated; and even (iv) specific file paths, folders, or file names of stolen trade secrets. *See* FAC, ¶¶ 4, 6, 9, 51-53, 56, 63-64, 69-70, 74-78, 89-90, 100. What is more, not only are some of these files trade secrets in-and-of themselves but, also, the compilation of stolen files—considered as a whole—also constitutes trade secrets, as summarized below. *See id.* ¶¶ 13, 63, 70, 91.

- **Jesus Gonzales Fernandez** downloaded "over 100,000 documents" including "engineering drawings, construction strategies, design management plans, bids and biddings strategies, project risk summaries, and pricing information," most of which are Plaintiffs' trade secrets. FAC ¶ 4. Some of these documents related to projects and bids on which he did not materially work. *See id.* ¶ 52. His file transfers—leading up to his unexpected November 19, 2024, resignation—contained trade secrets and took place on October 28-30, and November 4-8, 11-15. *See id.* ¶¶ 4, 53. In the two weeks or so before he resigned, he copied entire folders labeled "sensitive information"; "Sensitive Project No. 2"; "21 DSA TEMPLATES"; "DOWNLOADS FERRO LAPTOP"; "CONTRATOS INGENIERIAS"; "Correo"; "Jesus Correo"; "Sensitive Project No. 1"; and "DESKTOP FILES." *See id.* ¶ 56; *see also id.* ¶ 89.

- **Domingo Rodriguez Torregrosa** plugged in two storage devices (serial

[4] Additional safeguard measures include Plaintiffs' prompt, post-separation investigations in light of the Individuals' suspicious computing activity (*see id.* ¶¶ 5-6, 50, 59, 62, 69, 73), pre-suit demands for the return of stolen information (*see id.* ¶¶ 81, 86), as well as the eventual filing of this lawsuit seeking emergency relief (*see* ECF Nos. 1, 9-11).

numbers 4C530000280605123272 and WX62A44N277Y) on September 27 and 30, 2024. *See id.* ¶ 63. Using those devices, he "transferred numerous folders and subfolders that housed over 800 files" related to sensitive projects. *Id*. These "included a treasure trove of information about Plaintiffs' pricing, bidding strategy, project management and completion strategies, designs, budgets, cost information and summaries, payroll, privileged legal advice, risk analyses, confidential financial statements . . . confidential agreements, and executive presentations." *Id.* These stolen trade secrets include the following specific files: "[Sensitive Project No. 1] Longitudinal Study Meeting notes 20241001"; "2024.09.03_[Sensitive Project No. 1]_Stick_Diagram_v6 1.xlsx."; "Alternatives for [Sensitive Project No. 1].pptx"; "Cintra [Sensitive Project No. 2] Cost Scenarios.docx"; "[Sensitive Project No. 2] Strategic Plan v1.pdf"; "Due Diligence-[Sensitive Project No. 2]"; "Estimate [Sensitive Project No. 3]_Revision-May 6 2024.xlsx"; "Sensitive Project No. 3] I-5718.pdf"; "Estimate [Sensitive Project No. 3] (Analysis of [Sensitive Project No. 3[V_3.xlsx"; "Conceptual Unsolicited Proposal – [Sensitive Project No. 3] (Shared Version).pdf." *Id.*; *see also id.* ¶ 90.

- **Michael Valdes** used external storage devices to misappropriate "sensitive information relating to Plaintiffs' employees, human resource plans, and wage data." *Id.* ¶ 9. He had "access to sensitive information relating to staffing plans, various trainings, and wage data" which, on October 21, 2024, he used a storage device (serial number F90741050010202) to misappropriate. "Then, on November 11, 2024, [he used] a second external storage device" (serial number: WXU2E514URR) to "transfer[] more of those types of documents, including one particularly-sensitive file titled "Grand Employee Lists." *Id.* ¶ 69. The stolen files include, as another example, "a master employee roster"—that is not permitted to be removed from Plaintiffs' computer network and is essential to HR functions—and that "contains personal confidential information on [several employees] including social security numbers, date of birth, ethnicity, salary and home address[.]" *Id.* ¶ 70; *see also id.* ¶ 90.

- **Jose Luis Beltran** used a "JMicron" storage device "from February 13-18, 2025, to transfer what appears to be hundreds of thousands of documents." *Id.* ¶ 77. The files he misappropriated included "ANC's Construction and Design Contact List for the project, ANC videos, various purchase contracts, design and drawing files, project-related files (including plans, contracts, schedules, monthly cost data, accruals, and proposal data), technical submissions, subcontractor quotes, and tender phase documents." *Id.* He used that same device to transfer seemingly every "quote and proposal ANC received from potential vendors or

subcontractors during the bid phase of its project, each of which contains sensitive pricing (and other competitive) information." *Id.* 78; *see also id.* ¶ 90.

- **Maria Bregel Serna** used the same "JMicron" device to transfer files a day before submitting her resignation that included "subcontractors' monthly closures, project budgets, and employee wage information. She also transferred project layouts and designs." *Id.* ¶ 74. She used it again on February 14 and 16, 2025—days before her separation—to transfer "a contract for a large-scale project" as well as "further cost-related documents, procurement contracts, and various design files." On February 18 and 19, 2025—the eve of her separation—Ms. Serna transferred "more monthly closings, various contracts, procurement breakdown spreadsheets, procurement plans, supplier information, office budgets, comparative pricing spreadsheets, risk assessments, pricing quotes and estimates, and business opportunity matrices," in addition to "payroll data" which was apparently transferred using another "UDisk" storage device. *Id.* ¶ 76; *see also id.* ¶ 90.

Because of the magnitude of trade secrets transferred and retained without authorization, Plaintiffs and Acciona agreed to a *Forensic Protocol*—as directed by the *Consent Order* (ECF 63)—to further identify files containing Plaintiffs' trade secrets that the Individuals accessed while in Acciona's employ.

Acciona's Misconduct. The Individuals did not act independently to benefit only themselves but rather acted in concert to benefit each other as well as Plaintiffs' competitor, Acciona. *See* FAC ¶¶ 1, 8, 11, 13, 67-68, 71, 85-87, 101, 109, 113-115. Indeed, the Individuals' wrongful conduct was "taken at the direction of, or with the tacit approval of, Acciona" and "for Acciona's benefit." *Id.* ¶ 101. The Individuals have plugged into their Acciona computers storage devices that they used to misappropriate Plaintiffs' information. *See id.* ¶¶ 85, 87. Acciona has not denied this unlawful migration and—when confronted by Plaintiffs—took no remedial steps,

thereby necessitating litigation. *See id.* ¶¶ 85-88.

Acciona knowingly benefited from the Individuals' wrongful conduct. For example, Acciona "expropriate[ed] Plaintiffs' playbook" and used Plaintiffs' master employee list (which contained contact and compensation information) to poach Plaintiffs' other employees. *Id.* ¶¶ 13, 70-71, 91, 101. Through the Individuals, Acciona—at a minimum—has access to Plaintiffs' trade secrets and confidential information, which provide it with an unfair advantage, all while actively bidding and competing against Plaintiffs' for the same work. *See id.* ¶¶ 91-92. This creates irreparable harm. *See id*. ¶ 99.

LAW AND ARGUMENT

I. Plaintiffs allege sufficient "reasonable measures."

As threshold matter, Defendants' attack on Plaintiffs' "reasonable measures" is fatally flawed, as Defendants improperly seek a "quintessentially fact-specific" finding that is inappropriate *even under a summary judgment standard*,[5] to say

[5] *Camp Creek Hosp. Inns, Inc. v. Sheraton Franchise Corp.*, 139 F.3d 1396, 1410-1412 (11th Cir. 1998) ("Whether . . . information constitutes a trade secret is a question of fact."); *Rockwell Graphic Sys, Inc. v. DEV Indus., Inc.*, 925 F.2d 174, 179 (7th Cir. 1991) ("Only in extreme cases can what is a 'reasonable' precaution be determined on . . . summary judgment," as the issue depends on a "balancing of costs and benefits that will vary from case to case and so require estimation and measurement."); *Learning Curve Toys, Inc. v. Playwood Toys, Inc.*, 342 F.3d 714, 725 (7th Cir. 2003) ("Whether the measures taken by a trade secret owner are sufficient to satisfy the Act's reasonableness standard ordinarily is a question of fact for the jury."); *Prismhr, Inc. v. Worklio,* LLC, No. 18-22841, 2019 U.S. Dist. LEXIS 242604, at *22-24) (S.D. Fla. Feb. 8, 2019) (denying a motion to dismiss despite

nothing of Rule 12's relaxed standard. Courts routinely reject "reasonable measure" arguments at all pre-trial stages. *See Avnet, Inc. v. Wyle Labs, Inc.*, 437 S.E. 2d 302, 303 (Ga. 1993) ("There was evidence that the customer lists were not freely or widely disseminated and that certain employees to whom the information contained in the lists had been disclosed were required to sign agreements to keep the information secret. It is immaterial that some, but not all, employees were required to sign such agreements. Even in the absence of an express agreement, it is an implied term of an employment contract that an employee will not divulge a trade secret learned by virtue of his employment to a competitor[.]"); *Checkpoint Fluidic Sys. Int'l, Ltd. v. Guccione*, 888 F. Supp. 2d 780, 798 (E.D. La. 2012) ("Courts are extremely hesitant to grant summary judgment [much less motions to dismiss] regarding fact intensive questions and whether one took reasonable steps to protect its trade secrets."); *Pyro Spectaculars N., Inc. v. Souza*, 861 F. Supp. 2d 1079, 1091 (E.D. Cal. 2012) ("While PSI's security practices are not perfect and these issues can certainly be explored further in discovery and at trial, the court finds for purposes of this motion that PSI has made reasonable efforts to maintain the secrecy of the information[.]"); *Glynn v. Impact Sci. & Tech, Inc.*, 807 F. Supp. 2d 391, 435 (D.

---

minimal allegations on "reasonable measures" because "whether a party has taken reasonable steps under the circumstances . . . is a factual inquiry that cannot be resolved on a motion to dismiss").

Md. 2011), *aff'd*, 710 F.3d 209 (4th Cir. 2013) (rejecting a 'lack of reasonable measures' argument made on the grounds that, in two instances, former employees retained documents after departing, and noting measures need not be "fool proof," and this was a jury issue).[6]

Despite the combined weight of these federal decisions, Defendants persist in ignoring the well-plead reality of the measures taken to secure Plaintiffs' data. Bafflingly, in this vein, Defendants (i) emphasize potential "reasonable measures" that Plaintiffs do not allege they took, and (ii) focus on the absence of other, available "reasonable measures" that Defendants' seem to believe could or should have been taken, all while (iii) overlooking Plaintiffs' specific allegations. To embrace Defendants' proposed analysis would turn Rule 12 on its head.

For instance, Defendants primarily argue that "Plaintiffs do not even allege that any [Individuals] signed a nondisclosure agreement." *See* MTD at 15-20. While

[6] Here, a fact-intensive "reasonable measures" analysis must consider the tenure, sophistication, and rank of the Individuals, as well as the intuitive value of Plaintiffs' trade secrets. *See NW Airlines v. Amer. Airlines*, 853 F. Supp. 1110, 1116 (D. Minn. 1994) (noting that "[g]iven the level of sophistication and technical expertise of the employees . . . the court cannot say that as a matter of law the measures taken . . . did not give the employees reasons to know" the information should be protected). This is especially true for an HR manager like Valdes who was responsible for implementing Plaintiffs' policies. *See La Calhene, Inc. v. Spolyar*, 938 F. Supp. 523, 530 (W.D. Wis. 1996) ("It would be ironic . . . if defendant's failure to take proper measures to protect . . . confidential information and knowledge base inured to his benefit.").

the statement itself is technically truthful, this argument is nevertheless misleading. The law is clear—particularly under the GTSA (and outside the U.S. Second Circuit)—that a signed confidentiality or non-disclosure policy is ***not*** required to establish "reasonable measures." *See Candy Craft Creations, LLC v. Garntner*, No. 212-091, 2015 U.S. Dist. LEXIS 44646, at *54-58 (S.D. Ga. Mar. 31, 2015) (noting that "[e]mployers do not lose GTSA protection by sharing trade secrets 'with employees or other confidants who are legally obligated, by express or implicit agreement or by another duty imposed by law, to maintain its secrecy[,]'" and "confidentiality agreements are ***not required*** to garner protection under the GTSA" (emphasis added)); *see also Avnet*, 437 S.E. 2d at 306 (same).[7] Similarly, Defendants

[7] To argue otherwise on this discrete issue, Defendants cite *Kush Communications, LLC v. Lunex Telecom, Inc.*, No. 13-cv-03167, 2014 U.S. Dist. LEXIS 189254 (N.D. Ga. Sept. 12, 2014). But that case is inapposite, as it ***concerned a preliminary injunction***, and the court did not analyze "reasonable efforts" under Rule 12. *Id.* at *35 (noting that plaintiff's "opening brief [was] silent as to the specifics of [the] [reasonable] efforts" it took). The *Kush* court also considered that silence in its finding that the plaintiff failed to establish a likelihood of success on the issue of whether "persons with access to information concerning the [trade secret] were informed that Plaintiff considered such information to be a trade secret, or that such persons agreed, in writing or otherwise, not to disclose such information" *Id.* at *35. Accepting the FAC's allegations as true, the opposite is true here.

Defendants also cite New York federal cases, which, unlike cases from other circuits, appear to emphasize (even under Rule 12) signed confidentiality agreements. But those cases—*MedQuest Ltd.*; *Core SWX, LLC*; *Superb Motors Inc.*; and *Mason*—are distinguishable. *MedQuest* is discussed *infra* n. 9; and *Core SWX* and *Superb Motors Inc.* are distinguishable for largely the same reasons. Lastly, *Mason* concerned (i) the denial of an injunction and (ii) a situation wherein an

suggest that the Individuals were ignorant of, untrained on, or not in agreement with Plaintiffs' applicable policies (*see* MTD at 19). And, yet, Plaintiffs have clearly plead allegations to the effect that each Individual was bound by Plaintiffs' established "Corporate Code of Ethics," "Procedure for the Use of Technological Resources," and "Competition Policy," all which impose confidentiality obligations.[8] FAC ¶¶ 32-33. Further, the FAC explicitly alleges "Plaintiffs also train their employees, including all new hires, with access to confidential company documents that the documents are confidential and valuable to Plaintiffs and may not be disclosed to anyone outside of the Ferrovial family of businesses." *Id.* ¶ 35. Defendants' statements, then, that Plaintiffs have not "alleg[ed] that they communicated to the Individuals that any of the files at issue" contained trade secrets (MTD at 16) and that "[t]here are no plausible allegations the Individuals were

---

employee gave his employer a program he had developed before his new job without any written agreement concerning its use after his employment ended, making it factually inapplicable. 848 F. App'x 447, 450 (2d Cir. 2021).

[8] Courts recognize that—apart from standalone signed confidentiality agreements—confidentiality obligations can flow from any number of ***different sources***, including codes of ethics, manuals, or handbooks. *Genworth Fin. Wealth Mgmt. v. McMullan*, 721 F. Supp. 2d 122, 125 (D. Conn. 2010) (granting an injunction and noting that "[d]uring the hearing, the Plaintiff also presented evidence that the client information at issue was password protected and that the Defendants were subject to a Code of Ethics[.]"); *Computer Assocs. Int'l v. Quest Software, Inc.*, 333 F. Supp. 2d 688, 696 (N.D. Ill. 2004) (granting an injunction and weighing that the plaintiff had "[c]onfidentiality policies . . . set forth in employee manuals").

informed" about "or were trained on" policies (*id.* at 19) are simply incorrect, as is their reliance on *Diamond Power International, Inc. v. Davidson*; *In re Island Industries, Inc.*; and *MedQuest*.[9]

Beyond policies and training, Plaintiffs also allege that their confidential information is housed on "password-protected internal computer servers that can only be accessed by select employees who have a valid reason to review or use the

[9] *Diamond Power* concerned summary judgment, and the court did not analyze "reasonable efforts" under Rule 12. 540 F. Supp. 2d 1322 (N.D. Ga. 2007). The court in *MedQuest* weighed the absence of a signed non-disclosure agreement, but it also considered that the defendants were not bound by a general policy with a confidentiality provision, in distinct contrast to the allegations in this civil action. 2023 U.S. Dist. LEXIS 46830, at *13. The *MedQuest* plaintiffs also did not make additional allegations like the ones at issue here, including that the Individuals were trained on policies with confidentiality obligations, and that each time they logged into work computers, they acknowledged that their access was for a limited purpose and subject to Plaintiffs' policies.

Defendants also cite *Opus Fund Servs. (USA) LLC v. Theorem Fund Servs., LLC*—which is an outlier distinguished by at least one other case from the same court. *See Meridian Labs., Inc. v. OncoGenerix USA, Inc.*, No. 18-6007, 2020 U.S. Dist. LEXIS 84352, at *25 (N.D. Ill. May 13, 2020) ("The two district court decisions that defendant cites are not particularly analogous—in both cases, the alleged trade secrets were customer lists or other business information that was not obviously closely protected."). Lastly, Defendants uncritically cite *In re Island*, where the plaintiff "failed to allege the existence of its need-to-know policy in its complaint[,]" and also did "not demonstrate that it took any actions to protect its trade secrets, let alone reasonable actions." In contrast, the FAC contains detailed allegations on "reasonable measures," including allegations of the very type that the *Island* court indicated are sufficient to maintain a trade secret claim. 2024 U.S. App. LEXIS 5077, at *9 (collecting cases instructing that "alleged dissemination of information on a need-to-know basis and the imposition of confidentiality agreements can constitute reasonable measures").

information." *Id.* Further, "[m]any of Ferrovial's sensitive documents"—like the stolen "Grand Employee List," which "is never allowed to be removed from Ferrovial's computing network"—are "protected further still, such that only certain management-level employees within Ferrovial have the ability to access or modify" them. *Id.* ¶¶ 35, 70. In addition, "Plaintiffs are able to monitor employees' computing activity and do so in order to safeguard their trade secrets." *Id.* ¶ 35.

Taken together, Plaintiffs have more than sufficiently alleged confidentiality and access-limiting efforts to plead trade secret claims under Rule 12. For that matter, the same allegations would have entitled Plaintiffs to emergency injunctive relief, too, had the *Consent Order* not been entered. *See Deutsche Bank Sec. v. Pruitt*, No. 11-04434, 2012 U.S. Dist. LEXIS 203105, at *12-13 (N.D. Ga. Jan. 4, 2012) (granting injunctive relief and weighing that "Deutsche Bank's customer list is protected . . . . [T]he security of customer information is maintained by, among other methods, limiting access to computer data and hard copies, restricting access to only those IDs who have a need to know, and by instituting a confidentiality policy and requiring financial advisors and their office staff to abide by its requirements. These efforts to maintain secrecy are reasonable . . .").

Defendants also cherry-pick a slew of non-binding cases to identify other potential "reasonable measures"—like "exit policies," "mark[ing] . . . files as confidential," or "password-protect[ing]" computer systems—to make more Rule 12

"reasonable measure" arguments. MTD at 16-18. But none of these cases supports the conclusion that the absence of any such measure is fatal to a trade secret claim.

On the issue of "exit interviews," Defendants uncritically cite several cases to suggest that this a dispositive factor and not just one for a fact-finder to weigh at trial. *See* MTD at 10 & n.4. *DM Trans, LLC v. Scott* concerned an appeal of a denied preliminary injunction wherein the appellate court focused its analysis on the absence of "irreparable harm." 38 F.4th 608, 613. That case therefore is inapposite, though the *DM Trans* appellate court did instruct that "[c]ourts evaluate the question of whether efforts to keep information confidential were sufficient 'on a case-by-case basis, considering the efforts taken and the costs, benefits, and practicalities of the circumstances.'" *Id.* at 622, n. 5. The decision in *Balearia Caribbean Ltd.* is equally distinguishable, as it came after a full trial, and the only information at issue was a "template" that was "nothing more than a profit and loss statement in an excel format, which most courts have found is not protected under the DTSA." 2019 U.S. Dist. LEXIS 36868, at *21. And the remaining Illinois federal cases are also distinguishable because they do not concern Rule 12 but instead concern the denial of a preliminary injunction and summary judgment.[10]

[10] To deny a preliminary injunction, the *Abrasic 90* court noted the complete "absence of an articulated and developed confidentiality policy," as well as the fact that the employer "did nothing to train or instruct employees as to their obligation to keep certain categories of information confidential" and that information was shared with "suppliers or distributors" not required to keep it secret. *Abrasic 90*, 364 F.

Lastly, Defendants scoff at Plaintiffs' allegations that they restrict trade secret access with an even higher level of protection for certain files like the "Grand Employee Lists." *See* MTD at 19-20. Defendants cite a single case from the Eastern District of New York—*Negative, Inc. v. McNamara*—to diminish these reasonable efforts, even though the weight of authorities, including Defendants' own cited cases, recognizes that this constitutes "reasonable measures."[11] For example, in *Island Industries* (which Defendants cite), the appellate court provided the following string citation of cases wherein certain efforts—like maintaining trade secrets on an internal network with passwords—were sufficient:

> *Trans-Radial Sols., LLC v. Burlington Med., LLC*, No. 2:18-cv-656, 2019 WL 3557879, at *16 (E.D. Va. Aug. 5, 2019) (allegation of restricting access and disclosing information to defendants only on a need-to-know basis sufficient to survive motion to dismiss); *HTS, Inc. v. Boley*, 954 F. Supp. 2d 927, 944 (D. Ariz. 2013) (allegations that secrets were password protected and accessible only to certain employees sufficient); *Harsco Corp. v. Piontek*, No. 3:07-0633, 2008 WL 686217, at *8 (M.D. Tenn. Mar. 5, 2008) (code of conduct requiring confidentiality for employees, imposition of confidentiality

---

Supp. 3d at 900. Those facts are simply not applicable here, and the absence of an exit interview was, as it should be, just one area of a much larger focus. *CMBB* is also distinguishable, as it concerned a summary judgment motion, and the court weighed that – unlike this case – there was "no written policy or procedure as to" how the information at issue could be used. 628 F. Supp. 2d 881, 885.

[11] Notably, the *Negative* court was persuaded by the fact that, unlike Plaintiffs, their plaintiff did "not plead that it ever communicated to its freelancers what information they might encounter on Negative's electronic systems should (or should not) be kept confidential," which "strongly cut against its position" that the information at issue constituted trade secrets. *Id.* at *13-14.

> agreements in purchase orders, and use of physical obstructions to block the protected machinery from visitors in the building sufficient for preliminary injunction); *Phoenix Process Equip. Co. v. Capital Equip. & Trading Corp.*, No. 3:16-CV-024-CHB, 2022 WL 4687025, at *23-24 (W.D. Ky. Sept. 30, 2022) (deeming evidence of need-to-know policy and password protection, among other measures, sufficient to surpass summary judgment).

2024 U.S. App. Lexis 5077, at *9-10 (internal citations modified). The true import of these cases is that what constitutes "reasonable measures" is fact-intensive and not appropriate for resolution under Rule 12 given Plaintiffs' robust allegations.[12] *See* Section I.A., *supra*; *see also Amedisys Holding, LLC v. Interim Healthcare of Atl., Inc.*, 793 F. Supp. 2d 1302, 1311 (N.D. Ga. 2011) (finding reasonable measures taken where the employer, in part, "only transmitted [the information at issue] through its protected computer network and email system"); *Elec. Data Sys. Corp., v. Heinemann*, 493 S.E. 2d 132, 136 (Ga. 1997) (affirming determination of trade secret, in part, because employers' confidentiality agreements and limited access were reasonable); *Stone v. Williams Gen. Corp.*, 597 S.E. 2d 456, 459 (Ga. Ct. App. 2004) (finding that (i) reasonable efforts were made by restricting access to

[12] Whatever the allegations in the FAC, it seems Defendants would have sought dismissal under an ill-conceived Rule 12 motion regardless. In *Foulk Consulting Services v. Blazemeter, Inc.*, **the same counsel representing Acciona in this case unsuccessfully sought dismissal** where the plaintiff had "more than plausibly alleged that it took 'reasonable measures' to keep its software program secret," including having alleged the existence of executed non-disclosure agreements. No. 20-cv-11446, 2020 U.S. Dist. LEXIS 257749, at *11-12 (E.D. Mich. Nov. 16, 2020).

documents and instructing employees information should not leave; and (ii) that it was unnecessary for company to have a written policy on trade secrets to claim misappropriation), *rev'd on other grounds*, 614 S.E.2d 758 (Ga. 2005).

II. Defendants' "reasonable identification" argument creates a fictitious, heightened pleading standard (that Plaintiffs, nevertheless, meet).

Defendants next argue that Plaintiffs must do more to identify with "reasonable particularity/specificity" its trade secrets *at the pleading stage*. MTD at 20-27. Strawman arguments aside, the only issue the Court must decide on this point is, again, whether Plaintiffs have pled sufficient facts to state a claim for relief that is facially plausible. *See DynCorp Int'l v. AAR Airlift Grp., Inc.*, 664 F. App'x 844, 848 (11th Cir. 2016) ("[T]he plaintiff need only allege sufficient facts to plausibly show a trade secret was involved and to give the defendant notice of the material it claims constituted a trade secret."). And here, the FAC contains numerous, specific allegations sufficient to put Defendants on notice (even when considered against Defendants' erroneous heightened pleading standard) concerning the misappropriation of trade secrets.

A. No heightened pleading standard exists for trade secret claims, and the "particularity/specificity" issue is best left to discovery.

Notably absent from Defendants' own argument as to the correct "Legal Standard" (MTD at 12-13) is any case demonstrating that—***at the pleading stage***—trade secret claims are somehow subject to a heightened pleading standard. *See* Fed.

R. Civ. P. 9(b). And that is because no such heightened pleading standard exists. *See Foulk Consulting Servs.*, 2020 U.S. Dist. LEXIS 257749, at *12 (noting that "Defendants argue Plaintiff's allegations of a trade secret are not sufficiently specific," but "Defendants cite no binding caselaw from the Sixth Circuit or Supreme Court that mandates such specificity. Notably, the Federal Rules of Civil Procedure do not require heightened pleadings for trade secret claims.").[13]

To illustrate this point, the court in *EarthCam, Inc. v. OxBlue* Corp, noted that "[a] plaintiff is not required to disclose trade secrets in detail ***when pleading*** a claim for trade secrets misappropriation." No. 11-02278, 2012 U.S. Dist. LEXIS 191822, at *26 (N.D. Ga. Mar. 26, 2012) (emphasis added); *see also Water & Energy Sav. Corp. v. Minor*, No. 04-1785, 2005 U.S. Dist. LEXIS 48688, at *2 (N.D. Ga. May 9, 2005) (finding that plaintiff's list of general terms including customer contacts, customer data, proposals, strategic plans, projects, and technical procedures to describe alleged trade secrets was sufficient to state a claim for relief under GTSA); *Baker Petrolite Corp. v. Brent*, No. 09-7047, 2010 U.S. Dist. LEXIS 21317, at *4-5 (E.D. La. Mar. 8, 2010) ("BPC's complaint alleges all of the elements of a LUTSA

[13] *See also DynCorp Int'l*, 664 F. App'x at 848; *MMR Constr., Inc.*, 2023 U.S. Dist. LEXIS 76947, at *6 ("Essentially, Defendants urge the Court to assess MMR's DTSA claim under a heightened pleading standard, similar to that required of fraud claims under Rule 9. But, as MMR notes, the [Federal Rules of Civil Procedure] do not impose any such requirement, and the Court will not invent one[.]").

claim: a trade secret, misappropriation, and injury. The factual allegations are sparse and somewhat conclusory but Rule 8 continues to require only a 'short and plain statement of the claim' . . . *Twombly* does not create a heightened pleading standard . . . "); *Complete Logistical Servs., LLC v. Rulh*, 350 F. Supp. 3d 512, 517-521 (E.D. La. 2018) (denying dismissal where plaintiffs alleged theft of internal financial information, customer lists, and sales analyses); *Sentry Data Sys., Inc. v. CVS Health*, 361 F. Supp. 3d 1279, 1292-94 (S.D. Fla. 2018) (allegations of "proprietary configurations and data specifications of [plaintiff's] software" were sufficient). Georgia federal courts applying the GTSA are no different. *See Candy Craft*, 2015 U.S. Dist. LEXIS 44646, at *58.[14]

[14] The court in *Candy Craft* stated: "***Defendants appear [to argue] that any failure to define with specificity what constitutes the trade secret results in summary judgment. However, the only case the parties have raised discussing the particularity requirement under Georgia law suggests otherwise***. In *Diamond Power*, the court initially noted that the plaintiff had failed to identify what specific elements about its proprietary sootblower were 'trade secrets.' *Id*. But rather than . . . dismiss the case for this failure alone, the court, on its own initiative, whittled down the plaintiff's designation of trade secrets from 'everything' about the sootblower to a few discreet features . . . to be evaluated for trade secret protection. *Id*. Here, the Court need not identify Candy Craft's trade secrets with particularity on its behalf, because it did so in its response to Defendants' First Interrogatories. ***The trade secrets include***: (1) Plaintiff's fondant recipes; (2) the identity and quantity of ingredients . . . ; (3) the formula and process for mixing ingredients . . . ; (4) Plaintiff's financial data, financial plans, product plans; (5) actual and potential customer lists; (6) pricing information; . . .Particularly, viewing the evidence in a light most favorable to Plaintiffs, there can be no question that Defendants were aware that secrets (1) through (3) above were trade secrets . . . ***Thus, there is at least***

Defendants' misstatement of the law on this issue is perhaps due to its confusion over a "specificity" analysis that is typically a creature of *discovery*, not one of 12(b)(6) motions. Defendants once again cite numerous distinguishable cases (*see* MTD at 20-21) but fail to address the weight of jurisprudence in other trade secret cases, which find the "particularity/specificity" issue should be addressed, if at all, in *discovery*. *See Intelliclear, LLC v. ETC Glob Holdings, Inc.*, ("[f]ederal cases analyzing whether a plaintiff's trade secrets are described with 'sufficient particularity' ***typically arise in the battleground of discovery***." 978 F.3d 653, 662 (9th Cir. 2020) (emphasis added) (collecting cases)). The *Intelliclear* court reversed summary judgment on this issue, ordering additional discovery after finding that the district court "abused its discretion" by not allowing the trade secret plaintiff to refine its list of trade secrets, after discovery, given the nature of the case. *See id.* at 663-664.

Defendants' erroneous attempt to conflate a discovery issue with a heightened pleading standard is further revealed by its citation to *A&P Tech., Inc. v. Lariviere*, in which the court analyzed a request for injunctive relief and ordered discovery sequencing around the further identification of trade secrets, rather than dismissing

---

a material issue of fact regarding whether Plaintiffs sufficiently identified their trade secrets with particularity." *Id.* at *58 (emphasis added).

trade secret claims under Rule 12, as Defendants seek here. No. 17-534, 2017 U.S. Dist. LEXIS 211822, at *2-31 (S.D. Ohio Dec. 27, 2017). The *Lariviere* court ordered the plaintiff's allegations to be particularized before the defendant had to produce its own trade secrets. *Id.*[15]

And even if there were some "specificity" concern, the parties have already addressed it under the *Consent Order*. It cannot be overstated that, in this case, the parties have already agreed to a *Forensic Protocol*—which is customary in trade secret cases involving massive data theft—to further identify the information at issue. The *Forensic Protocol* is a process specifically designed to narrow the trade secrets at issue, and Defendants need no additional protection (in the form of, for example, more detailed factual allegations than those set forth in the FAC) beyond this court-supervised process. The concerns underpinning the "reasonable

[15] Other cases confirming this as a discovery issue and not a Rule 12 relaxed-pleading analysis include: *Zenimax Media, Inc. v. Oculus VR, Inc.*, 2015 U.S. Dist. LEXIS 179923, at *5 (N.D. Tex. Feb. 13, 2015) ("While the Court recognizes that Plaintiffs are not required in this jurisdiction to allege trade secret claims with a particular level of detail, the Court has in the past required such" under discovery rules); *JJ Plank Co., LLC v. Bowman*, 2018 U.S. Dist. LEXIS 123792, at * 9 (W.D. La. Jul. 23, 2018) (recognizing that whether additional, pre-discovery identification is warranted is fact-specific); *United Servs. Auto. Ass'n v. Mitek Sys., Inc.*, 289 F.R.D. 244 (W.D. Tex. 2013) (discovery motion); *Switch Commc'ns Group v. Ballard*, No. 11-285, 2012 WL 2342929 (D. Nev. June 19, 2012) (same); *DeRubeis v. Witten Techs., Inc.*, 244 F.R.D. 676 (N.D. Ga. 2007) (same); *AutoMed Techs., Inc. v. Eller*, 160 F. Supp. 2d 915 (N.D. Ill. 2001) (denying dismissal and granting a discovery order).

identification" line of cases—and what they aim to guard against—are just not present in this case.[16]

B. Plaintiffs have reasonably identified their trade secrets.

In any event, Plaintiffs have—under whatever standard—reasonably identified their trade secrets; and Defendants know exactly where to look for them. *See EarthCam, Inc.*, 2012 U.S. Dist. LEXIS 191822, at *24-28 (far less detailed allegations survived a motion to dismiss); *Water & Energy Sav. Corp*, 2005 U.S. Dist. LEXIS 48688, at *2 (same); *Candy Craft Creations, LLC*, 2015 U.S. Dist. LEXIS 44646, at *58 (same). Plaintiffs have gone to great lengths to identify—beyond what was required—the 'who, what, when, where and how' of Defendants' misappropriation of their trade secrets, including in detailed allegations that Defendants altogether ignore.

[16] Cases emphasizing a plaintiff's minimal burden to identify more than "broad categories" of trade secrets are often concerned with reining in competitively harmful discovery, where little to no effort has been made to identify trade secrets or allege misappropriation. *See Microwave Research Corp. v. Sanders Assoc., Inc.*, 110 F.R.D. 669, 673 (D. Mass. 1986) ("when a plaintiff cannot specify the trade secrets . . . which it claims were misappropriated, the test of whether or not such a plaintiff is entitled to the kind of broad discovery which Microwave seeks in the instant case . . . is whether there is a substantial factual basis for plaintiff's claim that the defendant has misappropriated its trade secrets. This requires something more than what is required in order to file a count alleging misappropriation of trade secrets"); *see also Coda Dev. S.R.O. v. Goodyear Tire & Rubber Co.*, No. 15-1572, 2019 U.S. Dist. LEXIS 202114, at *12 (N.D. Ohio Nov. 21, 2019) (requiring discovery "sequencing" after observing that "where the alleged disclosure of trade secrets was *entirely oral*, the danger of plaintiffs 'molding' their claims . . ." was of "particular concern.") (emphasis original). Here, no such danger exists.

Plaintiffs have also alleged that the compilation of its industry information, which is unique to Plaintiffs, is a trade secret. *See Compulife Software, Inc. v. Newman*, 959 F.2d 1288, 1314 (11th Cir. 2020) ("Even if quotes aren't trade secrets, taking enough of them must amount to misappropriation of the underlying secret at some point. Otherwise, there would be no substance to trade-secret protections for 'compilations,' ***which the law clearly provide*s**." (emphasis added)); *Cap Asset Rsch. Corp. v. Finnegan*, 160 F.2d 683, 686 (11th Cir. 1998) ("Even if all of the information is publicly available, a unique compilation of that information, which adds value to the information, also may qualify as a trade secret."); *Allstate Ins. Co. v. Fougere*, 79 F.4th 172, 189-190 (1st Cir. 2023) (instructing that under trade secret law a compilation of public and non-public information can be a trade secret); *see also* 18 U.S.C. 1983(3) ("trade secret" includes "compilations" of information).

In addition to mischaracterizing as 'vague' allegations that are, in fact, both detailed and specific, Defendants also attack other clearly-identified trade secrets to argue they can somehow never be a trade secret. *See* MTD at 24-26. For example, Defendants argue that under no circumstances can employee lists with compensation information be considered a trade secret. But the very cases they cite do not support this broad (and erroneous) proposition. *See Blades of Green, Inc. v. Go Green Lawn and Pest, LLC*, No. 22-00176, 2023 U.S. Dist. LEXIS 144241, at *8-9 (D. Md. Aug. 16, 2023) (distinguishable because, unlike here, the "precise information in the

employee-pay-related records [was] unclear," and the employee list was "retained in an email account, where the login information was left in the possession of former employees[.]"); *CAN Fin. Corp. v. Local 743 of Int'l Bhd. of Teamsters*, 515 F. Supp. 942, 946 (N.D. Ill. 1981) (noting that "an employee list may contain such extensive and detailed information that would so devastate a company if disclosed to the wrong person that it could be characterized as a trade secret"); *Pre-Paid Legal Servs. v. Harrell*, No. 06-00019, 2008 U.S. Dist. LEXIS 1773, at *28 (E.D. Okla. Jan. 8, 2008) (undercutting Defendants' argument by finding, after a trial, that the plaintiff's "roster" and "related financial and identifying information of associates constitute a trade secret."); *Humanitary Med. Ctr. Inc. v. Artica*, No. 23-01792, 2023 U.S. Dist. LEXIS 140646, at *3, 9 (M.D. Fla. Aug. 11, 2023) (enjoining the use of categories of information including misappropriated employee information).

Defendants' criticisms of "'designs,' 'costs,' etc." are equally unavailing. *See* MTD at 25-26. The GTSA defines "trade secret" to include "information, without regard to form, including, ***but not limited to***, technical or nontechnical data . . . a ***drawing***, a process, ***financial data***, financial plans, product plans, or a list of actual or potential customers or suppliers which is not commonly known by or available to the public[.]" (emphasis added). Whether some of the information at issue "may" pertain to information that belongs to a public entity (and may be subject to, for example, a public records request from a competitor) is a question of fact not ripe

for determination under Rule 12. *See Theragenics Corp. v. Dept. of Natural Resources*, 536 S.E. 2d 613, (Ga. Ct. App. 2000), *aff'd, Ga. Dept. of Natural Resources v. Theragenics Corp*., 545 S.E. 2d 904 (Ga. 2001).

Lastly, there is the issue of Defendants' allegations of insufficiency in Plaintiffs' allegation that specific file names and folders contain trade secrets. Simply put, the complaint is nonsensical in the context of Defendants' "reasonable identification" argument. MTD at 26-27. That is, if Defendants' grievance is not knowing what information is at issue, they need only look at those specific files and folders, which Plaintiffs clearly allege contain their trade secrets. The caselaw upon which Defendants rely to suggest that use of file names or folders to identify trade secrets is *per se* problematic under Rule 12 is easily distinguishable. *See Welter v. Med. Prof'l Mut. Ins. Co.*, No. 22-11047, 2023 U.S. Dist. LEXIS 70304, at *36-42 (D. Mass. Feb. 23, 2023) (where there were "few factual allegations" to "identify the nature of the alleged trade secrets at issue," and where the court concluded only that, based on the allegations, there was no "trade secret" status for complaints against a doctor filed with an administrative board); *Elsevier Inc. v. Dr. Evidence, LLC*, No. 17-cv-05540, 2018 U.S. Dist. LEXIS 10730, at *16-18) (S.D.N.Y. Jan. 23, 2018) (discussing impermissibly broad categories but not mentioning the use of file or folder names to specifically identify trade secret information). Simply put, these cases lend no actual authority to the MTD.

III. Plaintiffs allege improper "acquisition" and "use or disclosure."

Defendants next argue that Plaintiffs have not alleged improper "acquisition" or "use" of their trade secrets. *See* MTD at 27-30. [17]

Acquisition. As to "improper acquisition" misappropriation, Defendants suggest that, because the Individuals were still employed when they transferred (and retained for the benefit of a competitor) thousands of files and, therefore, still had access to them, their conduct is excused. *See* (*Id.*, p. 28) (complaining that Plaintiffs were not prohibited from using external storage devices during their employment). But that is not the law, particularly considering that the Individuals were employed in positions of trust and responsibility, with duties of loyalty, bound by Plaintiffs' policies protecting confidential information, and—importantly—that the Individuals ultimately hid their misappropriations.

Indeed, courts routinely find allegations that employees, like the Individuals, who violate confidentiality obligations by downloading trade secrets before resignation—and leave with that information—have engaged in "acquisition

[17] Defendants curiously state that "Improper means" is "defined as being an intentional wrongdoing." MTD at 28 (citing 18 U.S.C. 1839(6)). But "Improper means" is defined more fully to include "theft, bribery, misrepresentation, ***breach or inducement of a breach of a duty to maintain secrecy***, or espionage through electronic or other means." *Id.* § 1839(6) (emphasis added); Thus, "acquisition misappropriation" does not require a trade secret plaintiff to allege use or disclosure of the trade secrets, though Plaintiffs allege improper "use," also.

misappropriation." *See AUA Private Equity Partners, LLC v. Soto*, No. 17-08035, 2018 U.S. Dist. LEXIS 58356, at *20-21 (S.D.N.Y. Apr. 5, 2018) (explaining that, like here, improper acquisition through downloading information establishes liability and collecting cases where "[m]isappropriation by acquisition has been found under other state UTSAs in similar circumstances"); *ITR Am., LLC v. Trek, Inc.*, No. 16-00703, 2017 U.S. Dist. LEXIS 216172, at *20 (S.D. Miss. Sept. 26, 2017) (no dismissal where the employee "downloaded [] trade secrets after he had accepted a position with [his new employer], but before he resigned[.]"); *M-1 LLC v. Stelly*, 733 F. Supp. 2d 759, 773-74 (S.D. Tex. Aug. 17, 2010) (dismissal denied where the plaintiff alleged that "[i]n the days before [the defendant] notified [plaintiff] he was quitting, [the defendant] connected external devices to his [employer] laptop and transferred files to these devices from the laptop."); *Unified Brands, Inc. v. Teders*, 868 F. Supp. 2d 572 (S.D. Miss. June 19, 2012) (denying dismissal where employer alleged that former employee made copies of trade secrets at a time he knew he was planning to leave to compete).[18]

[18] Further, Defendants' reliance (*see* MTD at 29) on the outlying decision in *Angel Oak Mort. Sols. LLC v. Mastronardi*, 593 F. Supp. 3d 1234 (N.D. Ga. 2022) is misplaced. There, trade secret claims against two former-employees in that case were ***not*** dismissed, as the plaintiff "specifically allege[d]"—as in the FAC—that they "provided trade secrets" to a competitor. *Id.* at 1244-45. Trade secret claims against a different former employee were dismissed, but those claims concerned a handful of emails sent to a personal email account while still an employee. *See id.* at 1244. That is a far cry from the ***massive*** data transfers spelled out in the FAC using external storage devices. Regardless, as to that former-employee defendant, there

Use or disclosure. Plaintiffs have also adequately pled trade secret claims under 18 U.S.C. § 1839(B), referred to as "use or disclosure misappropriation." *See Lifesize, Inc. v. Chimene*, No. 16-cv-01109, 2017 U.S. Dist. LEXIS 64033, at *23-24 (W.D. Tex. Apr. 26, 2017) ("Acquisition by improper means is not the sole path to liability under TUTSA" because "[a] defendant can be liable for misappropriation . . . if, at the time of the unauthorized use or disclosure . . . , the defendant knew he obtained the information in circumstances giving rise to a duty to maintain its secrecy."). "Use or disclosure misappropriation" can be proved by establishing: (1) a trade secret; (2) was used or disclosed; (3) by a person; (4) who used improper

---

was no allegation that information in those emails was provided to, and used by, the competitor. *See id.* The same is not true of Plaintiffs' allegations in the FAC.

As to Defendants' reliance (*see* MTD at 29) on *eShares, Inc. v. Talton*, 727 F. Supp. 3d 463 (S.D.N.Y. 2023), the cited page in the MTD (page 493) does not exist. Regardless, that case guts Defendants' argument, as the court there ***denied*** a motion to dismiss and, on the issue of pleading "acquisition misappropriation," noted: " . . . the Court, based on a review of case law in the [SDNY], finds that transferring confidential information and trade secrets to a personal account can constitute acquisition by improper means under the DTSA [if]: (1) the employee was directed not to share the information outside of employer-issued devices—whether, for example, through a policy or employment-related contract; and (2) the employee transferred the information outside of an employer-issued device for an improper or illegitimate purpose." *Id.* at 475-76. There, "[the defendant] downloaded documents a few minutes after receiving an invitation for a meeting with [HR] and Carta's General Counsel to address a complaint [defendant] raised . . . before he was . . . placed on . . . leave. Carta also alleges that [defendant] has refused to return the alleged trade secrets. While a close call, these allegations are sufficient at this stage to suggest that the documents were downloaded for an improper . . . purpose." *Id.* The FAC's allegations are far stronger.

means to acquire it; or (5) who knew that the trade secret was acquired under circumstances giving rise to a duty to maintain the secrecy or limit its use. 18 U.S.C. § 1839(5)(B).

Having clearly alleged that the Individuals were obligated to maintain the confidentiality of their trade secrets, Plaintiffs also allege sufficient facts to—at a minimum—draw a reasonable inference that the Individuals all used or disclosed those trade secrets. *See Diamond Power Int'l, Inc. v. Davidson*, 540 F. Supp. 2d 1322, 1339 (N.D. Ga. 2007) ("[A] reasonable trier of fact could also conclude, based on the evidence that [the former employee] uploaded [plaintiff's documents] to the [new employer's] network, that [the former employee] disclosed the IOS Reports, the BOM Report, the Cost Data Report and the CMM's to [the new employer]."). That is, the Individuals would not have surreptitiously stolen Plaintiffs' trade secrets prior to joining a competitor, like Acciona, unless they were using them. This is further supported by the fact that many of the Individuals—acting in concert with Acciona—refused to return external storage devices despite formal pre-suit demands to do so, and at least some of those same devices were later plugged into Acciona computers. Inferences aside, the FAC also states that the Individuals have "used" the stolen information for the benefit of Acciona (thereby also "disclosing" it to

Acciona).[19]

The decision in *Molon Motor & Coil Corp v. Nidec Motor Corp.* is instructive. No. 16-cv-03545, 2017 U.S. Dist. LEXIS 71700, at *2-5 (N.D. Ill. May 11, 2017). There, an employee copied his former employer's motor design and engineer drawings, motor production inspection protocols, communication files with customers, and other confidential information. *Id*. at *4. The former employee then took a similar job with a competitor. *Id*. The former employer sued both its former employee and his new employer. Without identifying specific instances, the former employer "allege[d] (on information and belief) that [the former employee] 'unlawfully disclosed' the trade secrets he took from the memory stick to [the new employer] and that [the new employer] used and continues to use that information." *Id*. Like Defendants here, the new employer in *Molon Motor* argued, *inter alia*, that there was "no ground for inferring that it accessed or used any of the information [the former employee] pulled." *Id*. at *5. But the court rejected this illogical position and, considering the evidence of theft alleged against the employee, the direct competition between the parties, and the similarity of the former employee's work,

[19] Defendants seem to believe that the Court is insufficiently sophisticated to draw, from the FAC's numerous and specific allegations, the reasonable inference that the Individuals stole Plaintiffs' information shortly before their abrupt resignations so they could use it to benefit themselves and Acciona. After all, why else would the Individuals steal the information and evade questions about their conduct?

it found "enough to trigger the circumstantial inference that the trade secrets [at issue] inevitably would be disclosed by [the former employee] to [his new employer]." *Id.* at *17. Here, the Court need not rely solely on a theory of "inevitable disclosure," as Plaintiffs clearly allege the Individuals stole trade secrets, which they then used and disclosed to Acciona for its benefit, with its knowledge and approval.

IV. Plaintiffs have pled a claim against Acciona.

Plaintiffs allege that the Individuals' wrongful conduct was "taken at the direction of, or with the tacit approval of, Acciona" and "for Acciona's benefit." FAC ¶ 101. Plaintiffs further allege Acciona knowingly benefited from the [Individuals'] wrongful conduct—as examples, it "expropriate[ed] Plaintiffs' playbook," and poached Plaintiffs' other employees (armed with Plaintiffs' master employee list). *Id.* ¶¶ 13, 70-71, 91, 101. Further, through the Individuals, Acciona—at a minimum—has access to Plaintiffs' trade secrets, which provide it with an unfair advantage while bidding and competing against Plaintiffs for the same jobs. *See id.* ¶¶ 91-92. This creates a threat of irreparable harm. *Id.* ¶ 99. Plaintiffs also allege the Individuals plugged storage devices used to steal Plaintiffs' information into their Acciona computers.[20] *Id.* ¶¶ 85, 87. After learning this, Acciona took no remedial

[20] Acciona suggests Rodriguez may have plugged in a contraband external storage device into his Acciona-issued computer to access "personal files." MTD at 30 n.9. This hope is no basis to deny a claim under Rule 12's relaxed standard.

steps. *See id.* ¶¶ 85-88. Given the foregoing, Plaintiffs clearly allege that the Individuals used and disclosed Plaintiffs' trade secrets—including files and folders named in the FAC and identified through computer forensics—for the benefit of Acciona with its knowledge and approval. Taking these allegations as true, the Court must find they state a plausible claim for relief against Acciona.

Further, in addition to glossing over its independent liability, Acciona also fails to persuasively explain why it has no vicarious liability for the Individuals' misconduct once they were hired. *See Language Line Servs. v. Language Servs. Assocs.*, 944 F. Supp. 2d 775, 783 (N.D. Cal. 2013) ("The majority view, however, is that the UTSA does not preempt the *respondeat superior* doctrine."); *Newport News Indus. v. Dynamic Testing*, 130 F. Supp. 2d 745, 754 (E.D. Va. 2001) ("Instead, it is perfectly consistent to hold the employer liable for the infringing acts of its employee committed within the employee's scope of employment. The employer reaps the benefit of the employee's misconduct and therefore should be liable . . . ").[21] Courts in the Eleventh Circuit hold employers responsible for an employee's conduct done in the course of the employer's business and ***with a desire to benefit the employer***. *See Bennett v. U.S.*, 102 F.3d 486, 489 (11th Cir. 1996). Accordingly, in addition to pleading direct liability, Plaintiffs have at the very least

[21] This is especially true here, where Plaintiffs allege the Individuals conspired with Acciona to engage in the wrongful conduct at issue.

pled that Acciona is vicariously liable for the Individuals' misconduct while in Acciona's employ, as the Individuals acted to benefit themselves and Acciona.

V. Defendants' request to strike is improper, and leave to amend is required.

Defendants bury within the MTD a request to strike Plaintiffs' declarations verifying the FAC. *See* MTD at 14-15. This request is improper[22] and moot because the parties entered the *Consent Order* on Plaintiffs' request for emergency relief. That is, the declarations' viability has no consequence under Rule 12, where all Plaintiffs' allegations are accepted as true, with all inferences drawn in their favor, even without verification. The verifications nevertheless bolster Plaintiffs' position that their allegations are sufficient.

Finally, leave to amend must be "liberally permitted." *Melia v. LexisNexis Risk Sols., Inc.*, 2023 U.S. Dist. LEXIS 180905, at *15 (N.D. Ga. Oct. 6, 2023). In the unlikely event the Court grants Rule 12 relief (which, of course, it should not), denying Plaintiffs the opportunity to amend would be an abuse of discretion as no scheduling order is in place, and Plaintiffs have neither engaged in bad faith nor acted with any dilatory motive.[23]

---

[22] *See Chavez v. Credit Nation Auto Sales, Inc.*, 966 F. Supp. 2d 1335, 1344 (N.D. Ga. 2012) ("The Court has repeatedly explained that a motion to strike is not the proper vehicle for challenging matters not contained in pleadings[.]").

[23] Even Defendants' cases analyzing trade secret claims under Rule 12 recognize that leave to amend is required when dismissal is based on one of the MTD's discrete arguments. *See Angel Oak Mrtg. Sols. LLC*, 593 F. Supp. 3d at 1245

CONCLUSION

Wherefore, Plaintiffs ask the Court to deny the MTD or, alternatively, grant leave to amend.

Respectfully submitted, this 22nd day of July, 2025.

/s/ Joseph F. Lavigne
*Joseph F. Lavigne
*P.J. Kee
JONES WALKER LLP
201 St. Charles Avenue – 50th Floor
New Orleans, Louisiana 70170-5100
Telephone: 504-582-8000
Email: jlavigne@joneswalker.com
Email: pkee@joneswalker.com
Jones Walker, LLP

and

Chad V. Theriot
JONES WALKER LLP
3455 Peachtree Road NE, Suite 1400
Atlanta, GA 30326
Telephone: 404-870-7515
Email: ctheriot@joneswalker.cm

Counsel for Plaintiffs
***Admitted Pro Hac**

(allowing leave to amend); *IQVIA, Inc. v. Breskin*, No. 22-02610, 2023 U.S. Dist. LEXIS 47174, at *19 (E.D. Penn. Mar. 20, 2023) (same).

CERTIFICATE OF SERVICE

I hereby certify that on July 22, 2025, I electronically filed the foregoing pleading with the Clerk of Court using the CM/ECF electronic filing system, which will send notification of same to all counsel of record.

/s/ Joseph F. Lavigne
*Joseph F. Lavigne